

IMPERVA THREAT RESEARCH

Threat Intel Report: April 27-May 3, 2026

Countries



Top Tags

313 Team

PowMix

Xlabs_v1

ShinyHunters

Everest

Executive Summary

Actionable Information:

- **Initial access is increasingly driven by exposed services and configuration gaps:** Attackers are prioritizing externally accessible management interfaces, misconfigured services, and weak authentication flows as reliable entry points, reducing the need for complex exploit chains.
- **Service disruption is being operationalized as a monetization strategy:** Denial-of-service activity is evolving from opportunistic attacks into deliberate coercion mechanisms, where availability is leveraged to extract payment or apply pressure.
- **Botnet ecosystems are becoming more versatile and purpose-built:** Modern botnets are combining multiple capabilities—such as resource hijacking, disruption, and lateral movement—while also targeting specific platforms or communities for greater efficiency.
- **Third-party and supply chain exposure continues to expand organizational risk:** Attackers are consistently exploiting indirect access paths through vendors, integrations, and shared infrastructure, making partner ecosystems a primary attack surface.
- **Data theft is increasingly tied to extortion at scale:** Threat actors are focusing on large-volume data exfiltration with the intent to monetize through ransom demands or public leaks, rather than relying solely on resale or targeted exploitation.
- **State-aligned cyber activity remains focused on strategic access and persistence:** Advanced actors continue to target infrastructure and service providers to enable broader downstream access, reinforcing long-term espionage and influence objectives.
- **Barriers to executing advanced cyber operations are declining:** Improvements in automation and emerging technologies are making capabilities like vulnerability discovery and attack planning more accessible, increasing the potential attack volume and sophistication.

Outlook:

The current threat landscape shows clear convergence around scale, access, and leverage. Attackers are prioritizing scalable entry points—misconfigured services, third-party integrations, and centralized platforms—to maximize downstream impact, whether through disruption (DDoS), monetization (cryptomining, extortion), or intelligence collection (APT activity). At the same time, the blending of techniques—such as botnets capable of both financial exploitation and service disruption—signals a shift toward more efficient, multi-use attack infrastructure. Looking forward, organizations should expect continued growth in supply chain-driven breaches, extortion-backed operations, and targeted disruption of critical digital dependencies, with emerging technologies like AI further accelerating attacker capability development and reducing operational barriers.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 11,724% [CVE-2026-3844](#)

- The Breeze Cache plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'fetch_gravatar_from_remote' function in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

↑ 1,966% [CVE-2026-33017](#)

- Langflow is a tool for building and deploying AI-powered agents and workflows. In versions prior to 1.9.0, the POST /api/v1/build_public_tmp/{flow_id}/flow endpoint allows building public flows without requiring authentication. When the optional data parameter is supplied, the endpoint uses attacker-controlled flow data (containing arbitrary Python code in node definitions) instead of the stored flow data from the database. This code is passed to exec() with zero sandboxing, resulting in unauthenticated remote code execution.

↑ 1,650% [CVE-2025-53772](#)

- Deserialization of untrusted data in Web Deploy allows an authorized attacker to execute code over a network.

Recent Cyber Threats

cPanel Auth Bypass Opens Admin Access Window

+CVE

- A critical authentication bypass vulnerability, [CVE-2026-41940](#), allows attackers to gain unauthorized administrative access to cPanel & WHM instances without valid credentials. The flaw stems from improper validation in the authentication flow, enabling full control over hosting environments if exploited. Imperva telemetry indicates active scanning and exploitation attempts targeting exposed management interfaces. The impact is severe, as compromise enables attackers to manipulate websites, access sensitive data, and pivot further into infrastructure. Imperva customers are protected out-of-the-box.

313 Team Claims DDoS Extortion Against Canonical

+313 Team +Iran +DDoS

- The Iranian threat group [313 Team](#) claimed responsibility for a distributed denial-of-service (DDoS) attack that disrupted multiple Ubuntu-related services operated by Canonical, causing outages that affected package repositories and infrastructure relied on by developers globally. The group alleged it could sustain or escalate attacks unless payment was made, reflecting a

continued trend of DDoS-for-ransom operations. While the full technical scale was not independently verified, the incident highlights how attackers leverage service disruption as coercion rather than purely for visibility. The targeting of a major Linux ecosystem provider amplifies potential downstream risk to dependent services.

AI Models Reach Parity in Simulated Cyber Offense Testing

+AI +UK

- A study by the UK AI Security Institute found that advanced models such as [Claude Mythos](#) performed on par with competitors like GPT-5.5 in controlled cyberattack simulations. The testing evaluated capabilities such as vulnerability discovery and exploitation planning, showing increasing sophistication in AI-assisted offensive workflows. While not tied to real-world attacks, the findings raise concerns about dual-use risks as models improve. The primary impact is strategic, highlighting how AI could lower the barrier for developing cyberattack capabilities.

Botnet Exploits Jenkins Misconfigurations to Hit Gaming Servers

+Jenkins +Gaming +Botnet

- A newly observed botnet is exploiting [misconfigured Jenkins instances](#) to compromise systems and launch attacks against gaming infrastructure. Attackers leverage exposed Jenkins servers to deploy malicious payloads, which are then used to conduct DDoS attacks on game servers. The campaign highlights the continued risk of improperly secured DevOps tools being repurposed for large-scale attacks. Impact includes service disruption for gaming platforms and potential lateral movement within compromised environments.

PowMix Botnet Expands Multi-Vector Attack Capabilities

+PowMix +Botnet +Linux +Crypto +DDoS

- The newly identified [PowMix](#) botnet is actively targeting Linux systems, combining cryptomining with DDoS capabilities to monetize infections. It spreads through known vulnerabilities and weak credentials, enabling rapid propagation across exposed systems. Once deployed, PowMix can execute multiple attack types, increasing its utility for operators. The impact spans resource hijacking, degraded system performance, and potential use in coordinated attack campaigns.

North Korea Pushes Back on Cybercrime Allegations Amid Ongoing Activity

+North Korea +US +Crypto +Government

- [North Korea](#) publicly denied U.S. accusations of state-sponsored cyber operations, calling them politically motivated, while warning it would take “necessary measures” in cyberspace. The statement comes as U.S. authorities continue to attribute hacking campaigns, cryptocurrency theft, and global IT worker schemes to Pyongyang-linked actors. Sanctions have already been imposed on individuals and entities tied to these operations, which are believed to fund weapons programs. The incident reflects ongoing geopolitical tension where cyber activity remains a persistent and contested domain of state conflict.

Xlabs_v1 Botnet Targets Minecraft Server Ecosystem

+Xlabs_v1 +Botnet +Gaming +DDoS

- The [Xlabs_v1](#) botnet is specifically targeting Minecraft servers, leveraging infected systems to launch DDoS attacks against gaming hosts. The botnet exploits vulnerabilities and weak configurations to grow its node base, focusing on disrupting multiplayer environments. This targeted approach suggests attackers are prioritizing communities with centralized infrastructure and predictable traffic patterns. The impact is concentrated on service availability, causing downtime and degraded gameplay for affected users.

Data Breaches

Canvas Platform Breach Exposes Student Data at Scale

+ShinyHunters +Education

- Educational technology firm [Instructure](#), known for the popular learning tool Canvas, confirmed a cyberattack in which attackers stole user data, with the ShinyHunters group claiming responsibility. Exposed information includes names, email addresses, student IDs, and internal messages, while passwords and financial data were reportedly not compromised. The group claims up

to 275 million users across ~9,000 institutions may be affected, though full scope remains under investigation. The breach disrupted services and triggered credential resets, highlighting the risk concentration in centralized education platforms.

Security Vendor Trellix Hit by Source Code Repository Intrusion

+Cybersecurity

- [Trellix](#) disclosed that attackers gained unauthorized access to part of its internal source code repository. The company engaged forensic experts and law enforcement but has not identified the threat actor or entry vector. While no evidence currently shows code tampering or exploitation, exposure of source code poses significant downstream risk, including vulnerability discovery and potential supply chain attacks. The incident underscores that even security vendors remain high-value targets for intellectual property theft.

ADT Customer Records Leaked Following Extortion Campaign

+ShinyHunters +US +Security

- Home security provider [ADT](#) suffered a breach attributed to ShinyHunters, impacting approximately 5.5 million individuals. Attackers accessed customer and corporate data, including names, addresses, and partial Social Security or tax ID numbers, and later leaked an 11GB dataset after ransom demands were not met. No financial account data was compromised, but exposed PII increases risk of phishing and identity fraud. The incident reflects continued success of extortion-driven data theft campaigns targeting large consumer datasets.

French National ID System Breach Linked to Teen Hacker

+France +Government

- [French authorities](#) launched an investigation into a 15-year-old suspect accused of breaching a government identity database and attempting to sell stolen data online. The attacker allegedly offered 12–18 million records containing sensitive citizen data from the national ID agency (ANTS), including passport and license information. The breach triggered nationwide alerts warning citizens of potential fraud and phishing risks. The case highlights both insider-scale access risks and the growing role of low-age actors in high-impact breaches.

China-Linked Salt Typhoon Targets IBM Subsidiary in Italy

+Salt Typhoon +China +Italy +IT

- A breach at [Sistemi Informativi](#), an Italian IBM subsidiary which manages IT infrastructure for public and private entities, has been linked to the China-associated threat group Salt Typhoon. The intrusion raised concerns about potential access to sensitive systems supporting government and enterprise operations. While IBM confirmed containment, the incident highlights the strategic targeting of infrastructure providers to enable broader espionage access. The breach underscores Europe's exposure to advanced persistent threat (APT) campaigns targeting digital supply chains.

Third-Party Breach at Citizens Bank Exposes Customer Financial Data

+Financial Services +US +Everest

- A data breach impacting [Citizens Bank](#) customers has been linked to the ransomware group Everest, which claimed to have exfiltrated sensitive data and published samples on its leak site. The incident originated from a compromised third-party vendor, with exposed information including names, addresses, and bank account numbers, data that could enable fraud like check forgery. While the bank stated only a limited number of customers were affected and core systems were not breached, lawsuits allege broader exposure and negligence. The attack highlights continued targeting of financial institutions through supply chain weaknesses rather than direct intrusion.

Vimeo Breach Tied to Third-Party Analytics Supply Chain Attack

+ShinyHunters +Software

- [Vimeo](#) confirmed that attackers accessed user and customer data via a breach of third-party analytics provider Anodot, with ShinyHunters claiming responsibility. Exposed data includes email addresses, video metadata, and technical information, but not login credentials, payment data, or video content. The attackers are attempting extortion, threatening to leak stolen data if ransom demands are not met. The incident highlights continued exploitation of SaaS integrations and analytics platforms as entry points into enterprise environments.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs– including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.